

# ARITMÉTICA I

Adolfo Quirós

COMPLEMENTOS PARA LA FORMACIÓN DISCIPLINAR  
EN MATEMÁTICAS  
Curso 2010-2011

# UNA FÓRMULA BIEN CONOCIDA

Demostrar que para todo número natural  $n \geq 1$

$$1 + 2 + 3 + \dots + n = \frac{(n-1)(n+2)}{2}.$$

## Demostración por inducción.

El principio de inducción se basa en los **Axiomas de Peano**, que caracterizan el conjunto  $\mathbb{N}$  de los números naturales.

## AXIOMAS DE PEANO (RELACIÓN = MÁS...)

- 1  $0 \in \mathbb{N}$ .
- 2 Existe una función  $S : \mathbb{N} \rightarrow \mathbb{N}$ . Es decir, para cada  $n \in \mathbb{N}$  existe un único  $S(n) \in \mathbb{N}$ , el **sucesor de  $n$** .
- 3 Para todo  $n \in \mathbb{N}$ ,  $S(n) \neq 0$
- 4  $S(m) = S(n) \implies m = n$ . Es decir,  $S$  es inyectiva.
- 5 **El axioma de inducción** Si  $K$  es un conjunto tal que
  - $0 \in K$ ,
  - para todo  $n \in \mathbb{N}$ , si  $n \in K \implies S(n) \in K$ ,entonces  $\mathbb{N} \subset K$ .

Por inducción podemos demostrar **fórmulas**:

$$1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}.$$

$$1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

$$\sum_k^n k \cdot k! = (n+1)! - 1.$$

**Desigualdades:** Para todo entero  $n > 4$  se tiene  $2^n > n^2 + 1$ .

**Teoremas:** Si  $A$  es un conjunto finito con  $\text{Card}(A) = n$  entonces  $A$  tiene  $2^n$  subconjuntos.

**Cosas extrañas:** Dado un conjunto  $C$  de caballos todos los caballos de  $C$  son del mismo color.

# DESCOMPOSICIÓN COMO PRODUCTO DE PRIMOS

Y también

## TEOREMA FUNDAMENTAL DE LA ARITMÉTICA (EXISTENCIA)

Dado un entero  $n > 1$  se puede escribir como

$$n = p_1 p_2 \dots p_r$$

donde  $p_1, p_2, \dots, p_r$  son primos, no necesariamente distintos.

- ¿Y  $n = 0$ ?
- ¿ $n = 1$ ?
- ¿Qué es un primo? ¿Es 1 primo?
- ¿Y si  $n \in \mathbb{Z}$  es quizás negativo?

Ejemplos:  $n_1 = 1306800$ ;  $n_2 = 1327103$

$$n_1 = 2^4 \cdot 3^3 \cdot 5^2 \cdot 11^2$$

$$n_2 = 1151 \cdot 1153$$

No es sólo cuestión de tamaños, **pero el tamaño importa.**

- ¿Es fácil encontrar primos?
- ¿Es fácil factorizar?

# MÁXIMO COMÚN DIVISOR Y MÍNIMO COMÚN MÚLTIPLO

## DEFINICIÓN VS CÁLCULO

- **¿Cómo se definen**  $(m, n) := m.c.d.(m, n)$  y  $[m, n] := m.c.m.(m, n)$ ?
- **¿Cómo se calculan**  $(m, n)$  : y  $[m, n]$

Ejemplo 1:

$$m_1 = 1306800 = 2^4 \cdot 3^3 \cdot 5^2 \cdot 11^2, \quad n_1 = 292500 = 2^2 \cdot 3^2 \cdot 5^4 \cdot 13$$

Ejemplo 2:

$$m_2 = 1292573, \quad n_2 = 1285667$$

**¿Cómo calculo  $(m_2, n_2)$  si no puedo factorizar?**

**¡Usando el Algoritmo de Euclides!**

# ¿CUÁNTOS NÚMEROS PRIMOS HAY?

¿Menos que enteros?

¿Más o menos que pares?

¿Más o menos que cuadrados?

¿Menos que racionales?

¿Menos que reales?